



ZZW
AF/2134

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
DALE E. GULICK
GEOFFREY S. STRONGIN

Examiner: P. Poltorak

Serial No.: 09/852,372

Group Art Unit: 2134

Filed: May 10, 2001

Att'y Docket: 2000.038300

For: SECURE EXECUTION BOX AND
METHOD

Customer NO. 023720

APPEAL BRIEF

Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF MAILING
37 C.F.R. 1.8

I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date below:

11/01/05
Date

Kathy Danas
Signature

Sir:

Appellant hereby submits this Appeal Brief to the Board of Patent Appeals and Interferences in response to the decision of the Primary Examiner mailed August 25, 2005. A Notice of Appeal was filed on September 6, 2005 and so this Appeal Brief is believed to be timely filed.

The Commissioner is authorized to deduct the fee for filing this Appeal Brief (\$500) from

Advanced Micro Devices, Inc.'s Deposit Account 01-0365/TT3756.¹

11/04/2005 NGUYEN1 00000038 010365 09852372

01 FC:1402 500.00 DA

¹ In the event the monies in that account are insufficient, the Director is authorized to withdraw funds from Williams, Morgan & Amerson, P.C. Deposit Account No. 50-0786/2000.038300.

I. REAL PARTY IN INTEREST

The present application is owned by Advanced Micro Devices, Inc. The assignment of the present application to Advanced Micro Devices, Inc., is recorded at Reel 11808, Frame 0464.

II. RELATED APPEALS AND INTERFERENCES

Appellant is not aware of any related appeals and/or interferences that might affect the outcome of this proceeding.

III. STATUS OF THE CLAIMS

Claims 1-10, 12-29, 31-48, and 50-52 are pending in the present application. Claims 1, 11-13, 15-16, 21, 30, 32-35, 38-41, 44-46, and 51-52 stand rejected under 35 U.S.C. 102(b) as being anticipated by the subject matter described on page 45 of the Hadfield publication, referred to hereinafter as Hadfield. Claims 17-18, 31, 37, and 50 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Hadfield in view of Official Notice. Claims 19-20 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Hadfield in view of Heald. Claims 24 and 43 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Hadfield in view of Vogt. Claims 23 and 42 were rejected under 35 U.S.C. 103(a) as being unpatentable over Hadfield in view of Anderson. Claims 2, 14, 22, and 37 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Hadfield in view of Aaro (U.S. Patent No. 6,662,020). Claims 3-10, 25-29, 36, and 47-48 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Hadfield in view of Angelo (U.S. Patent No. 6,581,162).

IV. STATUS OF AMENDMENTS

There were no amendments after the final rejections.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Claims 1, 21, 34, 39, and 40 set forth a plurality of operating modes including a secure operating mode and one or more secured assets coupled to a processor that may operate in one of the operating modes. Claims 1, 21, 34, 39, and 40 also set forth controlling access to the secured assets dependent upon the operating mode of the processor. In particular, claims 21, 34, and 39 set forth switching the computer system between a first operating mode and a second operating mode, where the second operating mode comprises a secure operating mode. Claims 21, 34, and 39 also set forth restricting access to the secured assets in response to the computer system being in the first operating mode and permitting access to the secured assets in response to the computer system being in the secure operating mode. Claims 1, 21, 34, 39, and 40 also set forth controlling access to the secure assets in the secure operating mode by providing access to a mailbox RAM configured to store input and output data.

In one exemplary embodiment, the mailbox RAM includes an inbox for storing input data for the one or more secured assets and an outbox for storing output data from the one or more secured assets. For example, one embodiment of mailbox RAM 415 includes two banks of RAM, such as 512 bytes each, for passing parameters into and out of the secure execution box 260. Parameters passed to or from the sub-devices included within the security hardware 370 are exchanged at the mailbox RAM 415. One bank of RAM 415, an inbox, is write-only to most of all of the computer system in most operating modes. Thus, parameters to be passed to the sub-devices included within the security hardware 370 may be written into the inbox. During

selected operating modes, such as SMM, both read and write accesses are allowed to the inbox. Another bank of RAM 415, an outbox, is read-only to most of all of the computer system in most operating modes. Thus, parameters to be received from the sub-devices included within the security hardware 370 may be read from the outbox. During selected operating modes, preferably secure modes, such as SMM, both read and write accesses are allowed to the outbox. See Patent Application, page 20, line 17 – page, 21, line 3 and Figure 5A.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Appellant respectfully requests that the Board review and overturn the seven rejections present in this case. The following issues are presented on appeal in this case:

- (A) Whether claims 1, 11-13, 15-16, 21, 30, 32-35, 38-41, 44-46, and 51-52 are anticipated by Hadfield;
- (B) Whether claims 17-18, 31, 37, and 50 are obvious over Hadfield in view of Official Notice;
- (C) Whether claims 19-20 are obvious over Hadfield in view of Heald;
- (D) Whether claims 24 and 43 are obvious over Hadfield in view of Vogt;
- (E) Whether claims 23 and 42 are obvious over Hadfield in view of Anderson;
- (F) Whether claims 2, 14, 22, and 37 are obvious over Hadfield in view of Aaro; and
- (G) Whether claims 3-10, 25-29, 36, and 47-48 are obvious over Hadfield in view of Angelo.

VII. ARGUMENT

A. Legal Standards

An anticipating reference by definition must disclose every limitation of the rejected claim in the same relationship to one another as set forth in the claim. *In re Bond*, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *In re Royka*, 490 F.2d 981, 180 U.S.P.Q. 580 (CCPA 1974). Second, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. That is, there must be something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination. *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561 (Fed. Cir. 1986). In fact, the absence of a suggestion to combine is dispositive in an obviousness determination. *Gambro Lundia AB v. Baxter Healthcare Corp.*, 110 F.3d 1573 (Fed. Cir. 1997). The mere fact that the prior art can be combined or modified does not make the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990); M.P.E.P. § 2143.01. Third, there must be a reasonable expectation of success.

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on Appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991); M.P.E.P. § 2142. A recent Federal Circuit case emphasizes that, in an obviousness situation, the prior art must disclose each and every element of the claimed invention, and that any motivation to combine or

modify the prior art must be based upon a suggestion in the prior art. *In re Lee*, 61 U.S.P.Q.2d 143 (Fed. Cir. 2002). Conclusory statements regarding common knowledge and common sense are insufficient to support a finding of obviousness. *Id.* at 1434-35. Moreover, it is the claimed invention, as a whole, that must be considered for purposes of determining obviousness. A mere selection of various bits and pieces of the claimed invention from various sources of prior art does not render a claimed invention obvious, unless there is a suggestion or motivation in the prior art for the claimed invention, when considered as a whole.

It is by now well established that teaching away by the prior art constitutes *prima facie* evidence that the claimed invention is not obvious. *See, inter alia, In re Fine*, 5 U.S.P.Q.2d (BNA) 1596, 1599 (Fed. Cir. 1988); *In re Nielson*, 2 U.S.P.Q.2d (BNA) 1525, 1528 (Fed. Cir. 1987); *In re Hedges*, 228 U.S.P.Q. (BNA) 685, 687 (Fed. Cir. 1986).

B. Claims 1, 11-13, 15-16, 21, 30, 32-35, 38-41, 44-46, and 51-52 are not anticipated by Hadfield.

Appellants note that the Examiner relies on a single page (page 45) of the Hadfield reference. Page 45 of Hadfield only provides a brief high-level summary description of a conventional Windows NT server that provides user accounts. To access a user account, a user must be validated by the system by providing a valid name and password. However, Hadfield does not describe or suggest a plurality of operating modes including a secure operating mode. Hadfield also fails to teach or suggest one or more secured assets coupled to a processor that may operate in one of the operating modes. The Examiner alleges that “files” may be secure assets. However, the Examiner provides no record support for this conclusory statement and Hadfield does not teach or suggest that “files” may be secure assets. Hadfield also fails to teach or

suggest a mailbox RAM that includes an inbox for storing input data for the one or more secured assets and an outbox for storing output data from the one or more secured assets.

For at least the aforementioned reasons, Appellants respectfully submit that the present invention is not anticipated by Hadfield and request that the Examiner's rejections of claims 1, 11-13, 15-16, 21, 30, 32-35, 38-41, 44-46, and 51-52 under 35 U.S.C. 102(b) be REVERSED.

C. Claims 17-18, 31, 37, and 50 are not obvious over Hadfield in view of Official Notice.

As discussed above, Hadfield fails to teach or suggest many limitations of the various embodiments of the inventions set forth in independent claims 1, 21, 34, and 40. Claims 17-18 depend from independent claim 1, claim 31 depends from independent claim 21, claim 37 depends from independent claim 34, and claim 50 depends from independent claim 40. In rejecting claims 17-18, 31, 37, and 50, the Examiner takes Official Notice that it is old and well-known to provide a predetermined response in lieu of data. Appellants note that the Examiner has failed to provide any record support for this conclusory statement.

Moreover, even if one accepts the Examiner's unsupported conclusory statements, the Examiner's Official Notice fails to remedy the fundamental deficiencies of Hadfield. To the contrary, the Examiner's conclusory statement does not even attempt to teach or suggest a plurality of operating modes including a secure operating mode. The Examiner's conclusory statement also fails to teach or suggest one or more secured assets coupled to a processor that may operate in one of the operating modes. The Examiner's conclusory statement also fails to teach or suggest a mailbox RAM that includes an inbox for storing input data for the one or more secured assets and an outbox for storing output data from the one or more secured assets.

For at least these reasons, Appellants respectfully submit that the present invention is not obvious over Hadfield in view of the Examiner's unsupported Official Notice. Appellants request that the Examiner's rejections of claims 17-18, 31, 37, and 50 under 35 U.S.C. 103(a) be REVERSED.

D. Claims 19-20 are not obvious over Hadfield in view of Heald.

As discussed above, Hadfield fails to teach or suggest many limitations of the various embodiments of the inventions set forth in independent claims 1. Claims 19-20 depend from independent claim 1. In rejecting these claims, the Examiner, relies on Heald to describe a battery to provide reserve power. However, Heald fails to remedy the fundamental deficiencies of Hadfield. In particular, Heald fails to teach or suggest a plurality of operating modes including a secure operating mode. Heald also fails to teach or suggest one or more secured assets coupled to a processor that may operate in one of the operating modes. Heald further fails to teach or suggest a mailbox RAM that includes an inbox for storing input data for the one or more secured assets and an outbox for storing output data from the one or more secured assets.

For at least these reasons, Appellants respectfully submit that the present invention is not obvious over Hadfield in view of Heald. Appellants request that the Examiner's rejections of claims 19-20 under 35 U.S.C. 103(a) be REVERSED.

E. Claims 24 and 43 are not obvious over Hadfield in view of Vogt.

As discussed above, Hadfield fails to teach or suggest many limitations of the various embodiments of the inventions set forth in independent claims 21 and 40. Claims 24 and 43 depend from independent claims 21 and 40, respectively. In rejecting these claims, the Examiner

relies on Vogt to describe a monotonic counter. However, Vogt fails to remedy the fundamental deficiencies of Hadfield. In particular, Vogt fails to teach or suggest a plurality of operating modes including a secure operating mode. Vogt also fails to teach or suggest one or more secured assets coupled to a processor that may operate in one of the operating modes Vogt further fails to teach or suggest a mailbox RAM that includes an inbox for storing input data for the one or more secured assets and an outbox for storing output data from the one or more secured assets.

For at least these reasons, Appellants respectfully submit that the present invention is not obvious over Hadfield in view of Vogt. Appellants request that the Examiner's rejections of claims 24 and 43 under 35 U.S.C. 103(a) be REVERSED.

F. Claims 23 and 42 are not obvious over Hadfield in view of Anderson.

As discussed above, Hadfield fails to teach or suggest many limitations of the various embodiments of the inventions set forth in independent claims 21 and 40. Claims 23 and 42 depend from independent claims 21 and 40, respectively. In rejecting these claims, the Examiner relies on Anderson describes a random number generator. However, Anderson fails to remedy the fundamental deficiencies of Hadfield. In particular, Anderson fails to teach or suggest a plurality of operating modes including a secure operating mode. Anderson also fails to teach or suggest one or more secured assets coupled to a processor that may operate in one of the operating modes. Anderson further fails to teach or suggest a mailbox RAM that includes an inbox for storing input data for the one or more secured assets and an outbox for storing output data from the one or more secured assets.

For at least these reasons, Appellants respectfully submit that the present invention is not obvious over Hadfield in view of Anderson. Appellants request that the Examiner's rejections of claims 23 and 42 under 35 U.S.C. 103(a) be REVERSED.

G. Claims 2, 14, 22, and 37 are not obvious over Hadfield in view of Aaro.

As discussed above, Hadfield fails to teach or suggest many limitations of the various embodiments of the inventions set forth in independent claims 1, 21, and 34. Claims 2 and 14 depend from independent claim 1, claim 22 depends from independent claim 21, and claim 37 depends from independent claim 34. In rejecting these claims, the Examiner relies on Aaro to describe a memory for storing data directly coupled to a display. However, Aaro fails to remedy the fundamental deficiencies of Hadfield. In particular, Aaro fails to teach or suggest a plurality of operating modes including a secure operating mode. Aaro also fails to teach or suggest one or more secured assets coupled to a processor that may operate in one of the operating modes. Aaro further fails to teach or suggest a mailbox RAM that includes an inbox for storing input data for the one or more secured assets and an outbox for storing output data from the one or more secured assets.

For at least these reasons, Appellants respectfully submit that the present invention is not obvious over Hadfield in view of Aaro. Appellants request that the Examiner's rejections of claims 2, 14, 22, and 37 under 35 U.S.C. 103(a) be REVERSED.

H. Claims 3-10, 25-29, 36, and 47-48 are not obvious over Hadfield in view of Angelo.

As discussed above, Hadfield fails to teach or suggest many limitations of the various embodiments of the inventions set forth in independent claims 1, 21, 34, and 40. Claims 3-10 depend from independent claim 1, claims 25-29 depend from independent claim 21, claim 36 depends from independent claim 34, and claims 47-48 depend from independent claim 40. In rejecting these claims, the Examiner relies on Angelo to describe a method for securely managing encryption information in a computer system that uses a secure mode of operation and a normal mode of operation. However, Angelo fails to remedy the fundamental deficiencies of Hadfield. In particular, Angelo fails to teach or suggest a plurality of operating modes including a secure operating mode. Angelo also fails to teach or suggest one or more secured assets coupled to a processor that may operate in one of the operating modes. Angelo further fails to teach or suggest a mailbox RAM that includes an inbox for storing input data for the one or more secured assets and an outbox for storing output data from the one or more secured assets.

For at least these reasons, Appellants respectfully submit that the present invention is not obvious over Hadfield in view of Angelo. Appellants request that the Examiner's rejections of claims 3-10, 25-29, 36, and 47-48 under 35 U.S.C. 103(a) be REVERSED.

VIII. CLAIMS APPENDIX

The claims that are the subject of the present appeal – claims 1-10, 12-29, 31-48, and 50-52 – are set forth in the attached “Claims Appendix.”

IX. EVIDENCE APPENDIX

There is no separate Evidence Appendix for this appeal.

X. RELATED PROCEEDINGS APPENDIX

There is no Related Proceedings Appendix for this appeal.

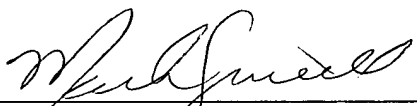
XI. CONCLUSION

In view of the foregoing, it is respectfully submitted that the Examiner erred in not allowing all claims pending in the present application, claims 1-10, 12-29, 31-48, and 50-52, over the prior art of record. The undersigned may be contacted at (713) 934-4052 with respect to any questions, comments or suggestions relating to this appeal.

Respectfully submitted,

Date: _____

11/1/05



Mark W. Sincell, Ph.D.

Reg. No. 52,226

WILLIAMS, MORGAN & AMERSON

10333 Richmond, Suite 1100

Houston, Texas 77042

(713) 934-7000

(713) 934-7011 (facsimile)

AGENT FOR APPELLANTS



CLAIMS APPENDIX

1. (Previously Presented) A system, comprising:

a processor configured to operate in an operating mode, wherein the operating mode is one of a plurality of operating modes including a secure operating mode;

one or more secured assets coupled to the processor;

security hardware configured to control access to the secured assets dependant upon the operating mode of the processor, wherein the security hardware is configured to allow access to the secure assets in the secure operating mode, and wherein the security hardware comprises a mailbox RAM configured to store input and output data, wherein the mailbox RAM includes an inbox for storing input data for the one or more secured assets and an outbox for storing output data from the one or more secured assets.
2. (Original) The system of claim 1, wherein the secured assets comprise one or more of the group consisting of:

a random number generator,

a secure management register,

a monotonic counter, and

a secure memory.
3. (Original) The system of claim 1, wherein the security hardware comprises:

an initiation register, wherein an entry in the initiation register is an indication to change

the operating mode of the processor to the secure mode.

4. (Original) The system of claim 1, wherein the secure operating mode comprises system management mode.
5. (Previously Presented) The system of claim 1, wherein the security hardware comprises:
a kick-out timer configured to provide an indication to the processor of when the processor is to exit the secure mode.
6. (Previously Presented) The system of claim 5, wherein the security hardware further comprises:
a re-initiation timer configured to provide an indication to the processor of when the processor is to exit the secure mode into a standard mode.
7. (Original) The system of claim 1, wherein the security hardware comprises:
a duration timer configured to operate while the processor is operating in the secure mode, wherein the duration timer is configured to provide an indication of how long the processor is in the secure mode.
8. (Original) The system of claim 7, wherein the security hardware comprises:
a kick-out timer configured to provide an indication to the processor of when the processor is to exit the secure mode.
9. (Original) The system of claim 8, wherein the kick-out timer and the duration timer comprise a single timer.

10. (Original) The system of claim 8, wherein the security hardware further comprises:
a re-initiation timer configured to provide an indication to the processor to re-enter the
secure mode.
11. (Canceled)
12. (Previously Presented) The system of claim 1, wherein the input data for the one or more
secured assets is addressed to the inbox of the mailbox RAM.
13. (Previously Presented) The system of claim 1, wherein the output data from the one or
more secured assets is retrieved from an address at the outbox of the mailbox RAM.
14. (Previously Presented) The system of claim 1, wherein the security hardware further
comprises:
access filters configured to provide input data or access requests to the inbox of the
mailbox RAM if the processor is operating in the secure operating mode, wherein
the access filters are further configured not to provide input data to the inbox of
the mailbox RAM if the processor is not operating in the secure operating mode,
and wherein the access filters are further configured to provide a predetermined
response in lieu of data upon receipt of said access requests if the processor is not
operating in the secure operating mode.

15. (Original) The system of claim 1, wherein the security hardware further comprises:
scratchpad RAM, wherein each of the one or more secured assets is configured to access
the scratchpad RAM for the storage of data.
16. (Previously Presented) The system of claim 1, further comprising:
a memory for storing data, wherein the memory is coupled to the processor and the processor is
configured to store and retrieve data from the memory in at least a portion of the plurality
of operating modes.
17. (Original) The system of claim 1, wherein the security hardware comprises:
access filters configured to provide access requests to one or more of the one or more
secured assets when the processor is operating in the secure operating mode,
wherein the access filters are further configured to provide a predetermined
response in lieu of data if the processor is not operating in the secure operating
mode.
18. (Original) The system of claim 17, wherein the security hardware further comprises:
access locks coupled to the access filters, wherein the access locks are configured to
disable the access filters in an unlocked mode.
19. (Original) The system of claim 1, further comprising:
a battery, wherein the battery provides reserve power to the one or more secured assets.

20. (Original) The system of claim 1, further comprising:
a battery, wherein the battery provides reserve power to the security hardware.
21. (Previously Presented) A method for providing access to secured assets in a computer system, the method comprising:
switching the computer system between a first operating mode and a second operating mode,
where second operating mode comprises a secure operating mode;
restricting access to the secured assets in response to the computer system being in the first operating mode; and
permitting access to the secured assets in response to the computer system being in the secure operating mode, wherein permitting access to the secured assets comprises reading output data from or writing input data to a mailbox RAM from which the secure assets write the output data and read the input data.
22. (Original) The method as set forth in claim 21, wherein the secure assets comprise a secure memory, and wherein permitting access to the secured assets comprises reading data from or writing data to the secure memory.
23. (Original) The method as set forth in claim 21, wherein the secure assets comprise a random number generator, and wherein permitting access to the secured assets comprises requesting a random number from the random number generator and receiving the random number from the random number generator.

24. (Original) The method as set forth in claim 21, wherein the secure assets comprise a monotonic counter, and wherein permitting access to the secured assets comprises requesting a value stored in the monotonic counter and receiving the value stored in the monotonic counter.

25. (Original) The method as set forth in claim 21, further comprising:
receiving a request to change the computer system from the first operating mode to the secure operating mode.

26. (Original) The method as set forth in claim 25, wherein receiving a request to change the computer system comprises providing an entry into an initiation register and asserting a control signal indicative of the entry in response to providing the entry.

27. (Original) The method as set forth in claim 26, wherein asserting the control signal indicative of the entry comprises providing a system management interrupt.

28. (Original) The method as set forth in claim 21, further comprising:
measuring a time period in which the computer system is in the secure operating mode; and
providing a control signal to the computer system to exit the secure operating mode in response to the time period in which the computer system is in the secure operating mode exceeding a predetermined length of time.

29. (Original) The method as set forth in claim 28, further comprising:
measuring a time period in which the computer system is out of the secure operating mode in
response to providing the control signal to the computer system to exit the secure
operating mode; and
providing a control signal to the computer system to re-enter the secure operating mode in
response to the time period in which the computer system is out of the secure operating
mode exceeding a predetermined length of time.

30. (Canceled)

31. (Original) The method as set forth in claim 21, further comprising:
receiving an access request for one of the secure assets; and
wherein restricting access to the secured assets comprises responding with a predetermined
response in lieu of data in response to receiving the access request for one of the secure
assets.

32. (Original) The method as set forth in claim 21, further comprising:
receiving an access request for one of the secure assets; and
wherein permitting access to the secured assets comprises providing the access request to the one
of the secure assets in response to receiving the access request for one of the secure
assets.

33. (Original) The method as set forth in claim 21, further comprising:

setting an access lock to an unlocked state; and

wherein permitting access to the secured assets further comprises overriding restricting access to the secured assets and providing the access request to the one of the secure assets in response to receiving the access request for one of the secure assets and in response to setting the access lock to the unlocked state.

34. (Previously Presented) A system, comprising:

means for switching the computer system between a first operating mode and a second operating mode, where second operating mode comprises a secure operating mode;

means for restricting access to the secured assets in response to the computer system being in the first operating mode; and

means for permitting access to the secured assets in response to the computer system being in the secure operating mode, wherein permitting access to the secured assets comprises reading output data from or writing input data to a mailbox RAM from which the secure assets write the output data and read the input data.

35. (Original) The system of claim 34, further comprising:

means for receiving a request to change the computer system from the first operating mode to the secure operating mode.

36. (Original) The system as set forth in claim 34, further comprising:
means for measuring a time period in which the computer system is in the secure operating mode; and
means for providing a control signal to the computer system to exit the secure operating mode in response to the time period in which the computer system is in the secure operating mode exceeding a predetermined length of time.

37. (Original) The system as set forth in claim 34, further comprising:
means for receiving an access request for one of the secure assets; and
means for responding with a predetermined response in lieu of data in response to receiving the access request for one of the secure assets.

38. (Original) The system as set forth in claim 34, further comprising:
means for receiving an access request for one of the secure assets; and
wherein the means for permitting access to the secured assets comprise means for providing the access request to the one of the secure assets in response to receiving the access request for one of the secure assets.

39. (Previously Presented) A system, comprising:
means for processing in an operating mode, wherein the operating mode is one of a plurality of operating modes including a secure operating mode;
one or more secured means coupled to the means for processing, wherein the one or more secured means comprise one or more of the group consisting of:

means for generating a random number or nonce;

means for storing secure management data;

means for generating a monotonic value; and

means for storing secure data; and

means for controlling access to the one or more secured means dependant upon the operating mode of the processor, wherein the one or more secured means comprise means for allowing access to the secure assets in the secure operating mode, and wherein the means for allowing access comprises a mailbox RAM configured to store input and output data, wherein the mailbox RAM includes an inbox for storing input data for the one or more secured assets and an outbox for storing output data from the one or more secured assets.

40. (Previously Presented) A computer readable program storage device encoded with instructions that, when executed by a computer system, performs a method of providing access to secured assets in the computer system, the method comprising:

switching the computer system between a first operating mode and a second operating mode, where second operating mode comprises a secure operating mode;

restricting access to the secured assets in response to the computer system being in the first operating mode; and

permitting access to the secured assets in response to the computer system being in the secure operating mode, wherein permitting access to the secured assets comprises reading output data from or writing input data to a mailbox RAM from which the secure assets write the output data and read the input data.

41. (Original) The computer readable program storage device as set forth in claim 40, wherein the secure assets comprise a secure memory, and wherein permitting access to the secured assets comprises reading data from or writing data to the secure memory.

42. (Original) The computer readable program storage device as set forth in claim 40, wherein the secure assets comprise a random number generator, and wherein permitting access to the secured assets comprises requesting a random number from the random number generator and receiving the random number from the random number generator.

43. (Original) The computer readable program storage device as set forth in claim 40, wherein the secure assets comprise a monotonic counter, and wherein permitting access to the secured assets comprises requesting a value stored in the monotonic counter and receiving the value stored in the monotonic counter.

44. (Original) The computer readable program storage device as set forth in claim 40, the method further comprising:
receiving a request to change the computer system from the first operating mode to the secure operating mode.

45. (Original) The computer readable program storage device as set forth in claim 44, wherein receiving a request to change the computer system comprises providing an entry into an initiation register and asserting a control signal indicative of the entry in response to providing the entry.

46. (Original) The computer readable program storage device as set forth in claim 45, wherein asserting the control signal indicative of the entry comprises providing a system management interrupt.

47. (Original) The computer readable program storage device as set forth in claim 40, the method further comprising:

measuring a time period in which the computer system is in the secure operating mode; and
providing a control signal to the computer system to exit the secure operating mode in response to the time period in which the computer system is in the secure operating mode exceeding a predetermined length of time.

48. (Original) The computer readable program storage device as set forth in claim 47, the method further comprising:

measuring a time period in which the computer system is out of the secure operating mode in response to providing the control signal to the computer system to exit the secure operating mode; and
providing a control signal to the computer system to re-enter the secure operating mode in response to the time period in which the computer system is out of the secure operating mode exceeding a predetermined length of time.

49. (Canceled)

50. (Original) The computer readable program storage device as set forth in claim 40, the method further comprising:

receiving an access request for one of the secure assets; and

wherein restricting access to the secured assets comprises responding with a predetermined response in lieu of data in response to receiving the access request for one of the secure assets.

51. (Original) The computer readable program storage device as set forth in claim 40, the method further comprising:

receiving an access request for one of the secure assets; and

wherein permitting access to the secured assets comprises providing the access request to the one of the secure assets in response to receiving the access request for one of the secure assets.

52. (Original) The computer readable program storage device as set forth in claim 40, the method further comprising:

setting an access lock to an unlocked state; and

wherein permitting access to the secured assets further comprises overriding restricting access to the secured assets and providing the access request to the one of the secure assets in response to receiving the access request for one of the secure assets and in response to setting the access lock to the unlocked state.